Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1726 07/17/15

~ First Look at Firebee! ~ People Are Talking! ~ Laserball 2015 ST!
~ GG1, New Google Glass? ~ Spamhaus Hacker Spared! ~ Commodore Comeback?
~ Right To Be Forgotten! ~ Nintendo’s Iwata Dies! ~ Darkode Dismantled!

~ Madonna Hacker Jailed! ~ Spam Levels Hit New Low ~ Gmail’s "Undo Send"!

-* FBI Worked with Hacking Team *-
-* Faceglória: Facebook Without the Sin *-
-* Microsoft Helps Crack Down on Child Porn! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, for a change, we have this week’s issue on time - perhaps even earlier than our "usual" release time! Don’t get all excited though, because it just so happens that I took a couple of days off from work this week (mini-vacation) and I managed to work on the issue throughout the week rather than try and get most of it done today!

It was nice to be able to relax a little bit this week; and the weather cooperated around here. It was warm, but not scorchers; and the nights were cool - no need for the AC blasting all night. Comfortable. But, that’s all going to change for the weekend, so I’m glad I was able to enjoy some seasonable weather for a little while.

So, let’s put this issue to bed, get it out early, and relax for the rest of the weekend (AFTER you finish reading the issue, of course!).

Until next time...

=~=~=~=

First of Many FireBee Contributions

by Fred Horvat

This is first of many semi-regular articles on owning a FireBee Computer. First a little about my Atari Computing background. I first got an Atari ST 1040 in 1992 with a SM124 monitor. I eventually owned many Atari computers including Megas, TTs, Falcons, and even a clone Milan040. My person favorite was an Atari TT030 with 4/4 RAM, TTM195 (19" Mono Monitor), internal IBM Server 270MB 7200RPM SCSI hard drive, SLM804 Laser Printer running MagiC Operating System, NVDI Screen/Printer accelerator, and Jinnee Desktop. This was my main computer for a period of time in the mid 90s. I really liked MagiC Operating System that I even purchased it (MagiCPC) for my Windows PC. Too bad the Atari market got too small for the developer to continue developing it. In the late 90’s early 2000s time frame I looked into MiNT Operating System as I did purchase MultiTOS for my TT before trying MagiC and liked it but found that it slowed the system down too much. MiNT 15 years ago didn’t have a simple method for installing

and setting all the required parts together. Well not free at least NAES 2.0 through Woller Systems did have a very simple setup program with all the required components. This was a commercial product that was in German and on a CD-ROM. None of these where show stoppers but did require the user to purchase a compatible CD-ROM reader, Cable, and CD-ROM driver software if you couldn't get one of the freeware drivers to work. I tried the free method of downloading all the pieces and putting them on floppies. I would then test my MiNT setup under Gemulator (Commercial Atari ST Emulator at the time http://www.emulators.com/gemul8r.htm) before attempting it on a real computer. I never did get a MiNT setup that I thought was working properly. My Unix understanding at the time was not very good either which hurt too. Two interesting pages on MiNT can be found here http://userpages.bright.net/~gfabasic/html/ers.htm and https://en.wikipedia.org/wiki/MiNT

Then in the early 2000's I was busy with work, family, and life in general and didn't touch an Atari Computer or fire up an Atari ST Emulator. Then in Spring 2014 I thought about running an Atari ST Emulation on my Mac. I had played with Aranym http://aranym.org/ and Hatari http://hatari.tuxfamily.org/ when they first came out on my BeOS PC but that was in the early 2000s and I didn't put a whole lot of effort into using either one of them. Now I wanted to attempt to setup an installation of MiNT with TCP/IP and Networking. I saw that there was a free prebuilt MiNT system called AFROS http://aranym.org/afros.html that was already done and even a Live CD if you wanted to test it out that way. AFROS is more of a MiNT install with a minimum amount of programs included for you to take a full test drive of Aranym running a fully working MiNT installation. I downloaded Aranym and AFROS to my Mac and tested it out. I got it running and Networking worked and I was surfing the Web with the included Highwire Web Browser. I was hooked all over again! I did more searching the Web and reading on the Atari-Forum http://www.atari-forum.com/ and saw that there was another fully setup MiNT installation called EasyARAMiNt https://sites.google.com/site/emaappsarch/news/finallythebetaishere EasyARAMiNT is a fully loaded MiNT setup with just about any piece of Atari software you could need to be fully functioning on an Atari Computer. I downloaded this and was amazed besides how inclusive but also how well it was put together.

I wanted to build my own my own Aranym MiNT setup as AFROS is very functional but not quite what I wanted while EasyARAMiNT is too much installed for me that it feels sluggish at times. I decided I wanted to use TOS 4.04 instead of the EmuTOS http://emutos.sourceforge.net/en/ I don't have anything against EmuTOS just that I am more familiar with TOS 4.04. I went and downloaded the EasyMiNT installer here http://atari.st-katharina-apotheke.de/home.php?lang=en&headline=EasyMiNT&texte=easymint
I then took an exist Aranym hard drive setup I got somewhere and formatted it and installed EasyMiNT there. EasyMint setup is very simple to use and get a fully working MiNT setup on a real Atari or a Virtual Machine (VM). In my case I chose a to use it on an Aranym VM. Now I had a solid starting point for my own customer MiNT setup. I did run into some problems with Host Drive Access that eventually by accident I figured out. If you do not use DHCP and hard code an IP Address for your Aranym VM during the installation with EasyMint, Host Drive Access does not work. Strange but true. Once that was taken care of I started installing my software and needed to install GDOS or NVDI to use certain software. I own both and like NVDI 5 better so when attempting to install NVDI my system would lock up. I messed around

but no matter what I did I couldn’t get past NVDI loading at start up. I was pretty much stuck at this point and my custom Aranym MiNT setup sat. About 6 months later on the Aranym User Mailing List someone asked about having the same issue and a solution was posted here https://lists.bobek.cz/pipermail/cz-bobek-lists-aranym-user/2015-January/005438.html

To Be Continued

=~=~=~=

->In This Week’s Gaming Section - Nintendo’s Iwata Dies at 55!
""""""""""""""""""""""""""""""""" Pre-Order Laserball 2015 ST!
Commodore Makes A Comeback?

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Nintendo’s Iwata, Who Led Through Successes, Woes Dies at 55

Satoru Iwata, who led Japanese video game company Nintendo Co. through years of growth with its Pokemon and Super Mario franchises, has died after a lengthy illness, drawing a flood of emotional tributes from game fans and industry rivals, the company said Monday. He was 55.

It said Iwata died Saturday of a bile duct tumor.

There was a torrent of sorrow online for Iwata as a person dedicated to entertaining others. On Twitter, fans thanked him for childhood memories and for bringing families together. On some Internet sites, an image of the flag in the Super Mario game was flying at half-staff. Nintendo America announced it was suspending social media activity for the day in remembrance of Iwata.

"He didn’t just create technology. He created a whole culture," said Nobuyuki Hayashi, a consultant and technology expert. "It wasn’t just a consumer product that he had delivered. He brought to people something that’s eternal, what people remember from when they were kids. He was special."

Iwata, president from 2002, died at Kyoto University Hospital. He had not been seen recently at game events, such as E3 in Los Angeles, where he was usually a participant.

Iwata led Nintendo’s development into a global company, with its hit Wii home console and DS handheld, and also through its recent troubles caused

by the popularity of smartphones.

His replacement was not immediately announced, but the company said star game designer Shigeru Miyamaoto will remain in the leadership team along with Genyo Takeda, who is also in the game development field.

Iwata had been poised to lead Nintendo through another stage after it recently did an about-face and said it will start making games for smartphones, meaning that Super Mario the plumber would soon start arriving on cellphones and tablets.

The falloff in appetite for game machines in the past few years was partly because people are increasingly playing games or doing social media and other activities on smartphones. Nintendo has repeatedly had to lower prices on gadgets to woo buyers. The company returned to profit in the fiscal year ended March 2015 after several years of losses.

Until the recent shift in strategy, company officials including Iwata had repeatedly rejected the idea of developing games for mobile devices, a market that they brushed off for years as irrelevant.

In March, Nintendo announced an alliance with Japanese mobile game company DeNA Co. to develop games for mobile devices.

Nintendo pioneered game machines since the 1980s, developing one of the first machines and the hit Game Boy hand-held device.

Its main rivals in the business are Sony Corp. with its PlayStation machines and Microsoft Corp. with the Xbox One. Both companies have done better in adapting to the era of online and mobile games.

"I am at a loss for words," said Ken Kutaragi, the former head of Sony Computer Entertainment. "I pay my respects to the extraordinary leadership of President Iwata, who truly loved games and powerfully showed the way for our industry."

Iwata succeeded Hiroshi Yamauchi, who ruled over the Kyoto-based company for half a century, transforming it from a traditional playing-card company to a technological powerhouse. Yamauchi died in 2013 at 85.

Iwata was picked with Yamauchi’s blessing, and Yamauchi remained adviser for many years. Iwata had been employed at an innovative software company before he was recruited as Nintendo chief. He was tapped as president at a surprisingly young age, in his early 40s, for a Japanese company.

Iwata was a respected and popular figure in the game industry, partly because he was relatively more approachable than executives at other Japanese companies, who tend to be aloof and rigid in demeanor.

As news of Iwata’s death spread online, condolences and virtual tributes emerged on social media and on Miiverse, Nintendo’s online community where users can post notes and drawings created with a Nintendo 3DS or Wii U stylus. Fans were circulating avatars called Mii in the likeness of Iwata, which already existed but were suddenly taking on special meaning.

"Halo" and "Destiny" developer Bungie posted a quote from Iwata’s 2005 talk at the Game Developers Conference on Twitter: "On my business card, I am a corporate president. In my mind, I am a game developer. But in my heart, I am a gamer."

On Twitter, personal homages were using the hashtags "ThankYouIwata" and "RIPSatoruIwata."

Iwata remained a presence in Nintendo promotional materials up until his death. While he had been absent from the Electronic Entertainment Expo for the past two years due to his health, Iwata appeared in both human and puppet form in a humorous video presentation streamed June 16 during the gaming expo.

Mark MacDonald, executive director at Tokyo-based 8-4, which consults about games, said Iwata was not afraid to be different and go against mainstream trends in games.

But he was also at one with game players, interacting with them, often using the Internet, in "this playful back and forth, like a David Letterman in your living room," MacDonald said in a telephone interview.

Miyamoto, the Nintendo game designer, said he was shocked and saddened.

"We will upkeep the development approach that we built with Iwata, and we in the development team hope to keep working as one to build toward the future," he said in a statement.

A funeral service will be held on July 17. Iwata is survived by his wife Kayoko. The company declined to disclose other details of his family.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Pre-Order Laserball 2015 Boxed Version for Atari ST

Hi to all ATARI ST Fans! Preparations are almost done. A boxed version of LASERBALL 2015 is coming soon. Including a shiny new box, a printed manual and an ATARI ST floppy disc.

I will have to have at least 25 Boxes being produced - as production of small amounts is relatively expensive the final price will be around 40 Euro + shipping. From now on I am taking pre-orders. If I get 15 or more pre-orders I will have the production started.
So pre-order now!

http://www.hd-videofilm.com/laserball/boxed-version/index.php

(3D Render of final design coming soon)

Legendary Company Commodore Makes A Comeback in the Form of a New Smartphone

Commodore, the emblematic computer tech brand of the 1980s is back with an Android smartphone that will allow users to play games from a whole other decade. Thanks to the installment of two emulators, games once played on the iconic C64 and Amiga PC will be available to nostalgic consumers.

The Commodore PET looks like a classic mid-range smartphone, 4G-compatible with double sim capacity. It features a 5.5-inch screen (1920x1080 pixels) and is equipped with a 1.7 GHz Mediatek 64-bit octa-core processor. It also includes a 13-megapixel camera able to film in high definition (1080p). Named PET, the phone pays tribute to the first ever Commodore computer launched in 1977.

The Commodore smartphone should hit stores between now and the end of July in Italy, Germany, Poland and France before becoming available elsewhere in Europe and in the United States. The price of the phone has not yet been announced.

Under the leadership of the company's creator Jack Tramiel and his associate Jay Gould, Commodore launched PET, its first computer, in 1977. The PET 2001 featured a small screen, a keypad and a cassette recorder. A few years later, the company encountered enormous success with the Commodore VIC-20, which was very affordable as well as simple and easy to use for the time. This model became the prototype for what would become the number one personal computer sold of the decade, the Commodore 64, launched in 1982. Aside from the computer's business applications, what made this computer so successful were the several thousand games available.

1985 marked the beginning of the Amiga computers (1000, 500, 600...) and ultimately the end of Commodore's hold on the PC market once the historic Window PC's were introduced.

Commodore's lack of progress in the following years coupled with the devastating failure of its CD32 console drove the company to bankruptcy in 1994. It was brought back to life in 2007 to market a new line of upmarket computers for gamers but had little success. Now in the hands of two Italian entrepreneurs, the company is targeting a new market while maintaining a reference to its past history.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

How Hacking Team and FBI Planned To Unmask A Tor User

The huge cache of internal files recently leaked from the controversial Italian surveillance software company Hacking Team has now revealed that the Federal Bureau of Investigation (FBI) purchased surveillance software from the company.

The leaked documents contains more than 1 Million internal emails,

including emails from FBI agent who wanted to unmask the identity of a user of Tor, the encrypted anonymizing network widely used by activists to keep their identities safe, but also used to host criminal activities.

In September last year, an FBI agent asked Hacking Team if the latest version of its Remote Control System (RCS), also known as Galileo - for which the company is famous for, would be capable to reveal the True IP address of a Tor user.

The FBI agent only had the proxy IP address of the target, as according to FBI, the target may be using Tor Browser Bundle (TBB) or some other variant. So, the agent wanted to infect the target's computer by making him download a malicious file.

"We'll need to send him an email with a document or PDF [attachment] to hopefully install the scout [Hacking Team's software]," the FBI agent wrote in the email.

In response to the FBI agent query, A Hacking Team staff member said that once the target's computer is infected, "if he is using TBB you will get the real IP address of the target. Otherwise, once the scout is installed you can inspect from the device evidence the list of installed programs."

So far, it isn't known whether the agents were succeeded in revealing the IP address of the target Tor user or who the target was, but internal emails clearly indicates that this FBI agent took full advantage of Hacking Team's service to unmask Tor users.

"[The FBI] continue to be interested in new features all the more related to TOR, [virtual private networks] VPN and less click infections," the same FBI agent said in other emails. "In the past their targets were 20 per cent on TOR, now they are 60 per cent on TOR."

Overall, the FBI has spent nearly $775,000 on Hacking Team's spy tools since 2011, Wired reports, although the internal emails indicate that the Remote Control System (RCS) tools were used as a "back up" for some other system the agency is already using.

Remote Control System (RCS), or Galileo, is the advanced and sophisticated spyware tool for which the Hacking Team is famous. It came loaded with lots of zero-day exploits and have the ability to monitor the computers of its targets remotely.

Hacking Team Spyware Preloaded With UEFI BIOS Rootkit To Hide Itself

Last week someone just hacked the infamous Hacking Team, The Italy-based cyber weapons manufacturer and leaked a huge trove of 400GB internal data, including:

Hacking Team is known for its advanced and sophisticated Remote Control System (RCS) spyware, also known as Galileo, which is loaded with lots of zero-day exploits and have ability to monitor the computers of its targets remotely.

Today, Trend Micro security researchers found that the Hacking Team "uses a UEFI (Unified Extensible Firmware Interface) BIOS Rootkit to keep their Remote Control System (RCS) agent installed in their targets' systems."

That clearly means, even if the user reinstalls the Operating System, formats the hard disk, and even buys a new hard disk, the agents are implanted after Microsoft Windows is up and running.

According to researchers, Hacking Team s rootkit malware is only able to target UEFI BIOS systems developed by Insyde and AMI vendors, used by the majority of computer and laptop manufacturers.

However, at this time researchers are not sure whether the malware can complete the rootkit installation without physical access to the target machine, as the installation requires BIOS flashing process that can t be done without rebooting into the machine into UEFI (Unified Extensible Firmware Interface) shell.

The BIOS rootkit analysis done by Trend Micro researchers was only made possible due to the Spyware source code leaked online in the Hacking Team data dumps.

So far, three Adobe Flash zero-day vulnerabilities and an Android zero-day exploit have been discovered from the Hacking Team leaked files, although this BIOS rootkit spreads more light on the team s activities.

The affected victims are yet unknown. However to keep yourself safe, we recommend you always to keep your BIOS up-to-date and protected by enabling password. Also, make sure to enable UEFI SecureFlash.

Microsoft Helps Web Services Crack Down on Child Porn

Microsoft wants to help other businesses crack down on child pornography. The software giant this week launched a cloud version of PhotoDNA, its technology that helps identify and remove child porn from the Internet. It is now available as a free service from the Azure Marketplace, allowing organizations to automatically detect child exploitation images on their services and report this illegal content to the National Center for Missing and Exploited Children and other law enforcement agencies.

Microsoft called the new cloud service a "major advance," which will make it easier and less expensive for companies to implement the technology. Before launching the cloud version, organizations needed to load PhotoDNA onto their own servers, and it required an in-house IT admin and engineering team to manage.

Big companies like Facebook and Twitter have been using PhotoDNA for years, but now it’s accessible for smaller Web services, like Flipboard, as well.

"Our community needs to trust that we do everything possible to stop the spread of illegal content, especially images of child sexual abuse," Flipboard’s Head of Platform Engineering, David Creemer, said in a statement. "Manually searching for a handful of illegal images among the millions uploaded and curated every day is simply an impossible task, so we looked for a solution and found it in Microsoft’s PhotoDNA."

The technology can essentially find and eradicate all copies of an offending image that appears across the Web. It converts images into a common black-and-white format and uniform size, then divides the images

into squares and assigns a numerical value that represents the unique shading found within each square. These numerical values together represent the "PhotoDNA signature" or "hash" of an image, which can then be compared against signatures of other images.

"While the technology cannot be used to identify a person or object in an image, nor can it be used to recreate an image, it can be used to find copies of a given image with incredible accuracy and at scale across the 1.8 billion images shared online every day, even when the images themselves have been altered," Microsoft said.

The new cloud service is free for qualified customers and developers, who can apply now to use it. At this time, it only works on images, not videos. For more info on the service, check out the video below and Microsoft’s FAQ.

Google took on a similar initiative in 2013, launching a shareable database that makes it easier for organizations to report and remove images of child sexual abuse from larger portions of the Web.

Most Google ’Right To Be Forgotten’ Requests Come From Everyday People

Newly leaked figures reveal that the vast majority of people who exercised their right to be forgotten by Google s services in Europe are everyday members of the public, with just 5 percent of requests coming from criminals, politicians and high-profile public figures.

Europe s highest court affirmed last year that people have the right to ask Google to remove certain results from its search engine, on the grounds that the information might be outdated or otherwise unfairly cast them in a negative light.

Google has protested the decision, arguing that removing links requires difficult value judgments and can go against the public interest. It has pointed to former politicians wanting posts removed that criticize their policies in office; serious, violent criminals asking for articles about their crimes to be deleted; bad reviews for professionals like architects and teachers; comments that people have written themselves (and now regret).

The figures suggest that requests from those first two categories, at least politicians and serious criminals have been minimal.

The Guardian newspaper discovered the numbers hidden in the source code for an archived version of Google s transparency report. The information has since been removed.

Google s original report provided the number of requests received and granted, but did not describe the nature of the requests in detail.

According to the Guardian, of the nearly 220,000 requests received as of March, more than 95 percent came from everyday citizens throughout Europe wanting links to private and personal information removed.

The requests included a woman whose name appeared in prominent news articles after her husband died, while another sought the removal of her address, The Guardian said. Another request came from an individual who

contracted HIV a decade ago.

The European court ruling said Google and other search engines should consider carefully whether information people want removed is irrelevant or outdated, and remove links unless there are compelling reasons not to do so, such as when the information might serve the public interest.

The leaked figures suggest Google is adhering to those principles. The company granted requests from everyday citizens at a higher frequency than those related to political or public figures or serious crimes. Google has granted nearly half of all private and personal requests, while for information tied to political and public figures, it granted less than a quarter of them.

In total, Google has received more than 280,000 requests to remove links since Europe s top court required Google and other search providers to do so last May.

Google still has complicated issues to weigh in determining whether information tied to requests from everyday people might still serve the public interest. But the numbers give an indication that it s not primarily criminals and politicians who want to use the ruling to erase the past.

A Google spokesman, in a statement, said the company has aimed to be as transparent as possible about its right to be forgotten decisions.

The data The Guardian found in our Transparency Reports source code does of course come from Google, but it was part of a test to figure out how we could best categorize requests, he said. The test was discontinued in March because the data was not reliable enough for publication, he said, but the company is working on ways to improve its transparency reporting.

Lad Who Attacked Spamhaus in DDoS Attack Avoids Prison, Given A Second Chance

Just over two years ago, we wrote about a massive DDoS attack against Spamhaus.

To explain, Spamhaus is a project that "tracks the internet’s spam senders" for the purpose of publishing blocklists of known spammers, and assisting law enforcement "to identify and pursue spammers worldwide."

And a DDoS is a Distributed Denial of Service attack, where you abuse lots of computers at the same time to flood someone’s server with purposeless traffic so it can’t keep up.

It’s a bit like getting all your friends to call up a takeaway joint at the same time, sit in the voicemail queue until they get answered, then to dilly-dally over what they want to order...

...before hanging up without buying anything.

The enquiries seem legitimate at first, but generate no business while at the same time keeping genuine callers at the back of a long queue.

Apparently, the attacks against Spamhaus were stirred up in a controversy called Stophaus, in which a countercultural posse of internet users

discussed taking out Spamhaus.

The Stophaus schemers, it seems, wanted to teach Spamhaus some kind of lesson for daring to take a stance against spam.

And so they attacked.

The trick they used is called DNS amplification, and it works like this.

DNS is the system that converts (amongst other things) internet names such as www.example.com into internet numbers such as 93.184.216.34.

DNS servers fall into three loose categories:

Ones that run on your router at home to service your home network, which simply relay your queries unaltered onwards to your ISP, or some other public server like Google's well-known 8.8.8.8.

Ones that organisations run as their own official DNS servers to give so-called authoritative answers to queries for the domains they own.

Ones that will accept your queries, reply immediately if they have the answer cached already, or else recursively (a fancy word for "in their turn") ask the authoritative servers on your behalf, cache the result for everyone else, and reply to you.

Most recursive servers aren't public, unlike Google's 8.8.8.8, because they end up doing a lot of work and carrying a lot of traffic.

So recursive servers are usually restricted to customers of a specific ISP, or to computers inside your company, or some other handily circumscribed set of users.

Or, if they're open to the public, they are carefully managed to prevent abuse.

One sort of abuse is to make multiple small requests to a recursive server such that each request provokes a much bigger request-and-reply from the authoritative server belonging to your victim.

Small requests turning into large ones is where the name amplification comes in.

In theory, amplification attacks should be hard to do, because the majority of DNS servers aren't supposed to be recursive in other words, they shouldn't pass on requests willy-nilly to other people's servers at all.

The problem was, at least when the Stophaus attack was carried out, that lots and lots of home routers perhaps 20 million or more were misconfigured to act as full-blown recursive servers for the whole world, as well as plain-old relay servers for the owner's home network.

So the Spamhaus attackers had millions of misconfigured DNS servers at their disposal that they could use to turn millions of modest and innocent-looking outbound DNS requests from their attack zombies into much larger amounts of DNS request-and-reply traffic, all of it aimed at Spamhaus.

According to reports, Spamhaus's DNS servers were subjected to traffic

peaks of 300Gbit/sec, the sort of attack that quickly gets not only disruptive but expensive.

Within a month or so, a 16-year-old was arrested for allegedly taking part in the Stophaus attack scene.

He couldn’t be named, being under 18, but he did put his hand up and plead guilty the following year to a bunch of offences.

At the time, those offences were reported as including money laundering and child abuse, with sentencing deferred until 2015.

The guilty party, having now turned 18, has recently been sentenced in Southwark crown court, and named as Seth Nolan Mcdonagh.

It sounds as though he wasn’t just a piracy-loving activist-leaning youngster who fell in with older hacker/cracker types and went along for the ride.

The BBC’s report suggests that Mcdonagh, who went by "narko" online, would take money to attack named websites, making him a sort of DDos gun-for-hire.

In fact, "narko" apparently had £72,000 (then about $105,000) in the bank at the time of the attacks not a bad nest-egg for a 16-year-old plus 1000 stolen credit card numbers on his computer.

Nevertheless, the court has given him a chance to reform without going to prison: he’s been sentenced to 240 hours of community service.

Let’s hope Mcdonagh, now legally an adult, takes this as an opportunity, not a lucky escape.

U.S. Says Computer Hacking Forum Darkode Dismantled, 12 Charged

The Federal Bureau of Investigation and law enforcement agencies from around the world have shut down Darkode, an international online forum used by cybercriminals, and brought charges against 12 people linked to the site, the U.S. Justice Department said on Wednesday.

"Darkode represented one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world," U.S. Attorney David Hickton said in announcing the charges in Pittsburgh.

Madonna Hacker Who Leaked Songs Sentenced to 14 Months

A 39-year-old Israeli man accused of leaking online several songs stolen from the pop star Madonna has been sentenced to 14 months in jail, after a reaching a plea agreement with authorities.

Adi Lederman, an aspiring singer and former contestant on the Israeli TV show "A Star Is Born," admitted that he had hacked several artists

including Madonna, and leaked unreleased songs online for profit.

Lederman was arrested in January after a joint investigation by the FBI and Israeli police.

Songs stolen from the private cloud accounts of several of Madonna’s associates and her manager were leaked online in December 2014, which she later released on her album "Rebel Heart."

Court documents showed that Lederman didn’t make much money from selling the songs to two accomplices - no more than $1000.

At the time of Lederman’s arrest, Madonna wrote on her website that she was grateful to the FBI and Israeli investigators for arresting the hacker responsible for the invasion of her privacy and professional work.

Like any citizen, I have the right to privacy. This invasion into my life - creatively, professionally, and personally remains a deeply devastating and hurtful experience, as it must be for all artists who are victims of this type of crime.

She also said in media interviews that the theft of her songs, and other material from her computer including images, constituted "a form of terrorism" and "artistic rape."

The Madonna hacking came at time when celebrity hacks had reached a crescendo - just a few months after the leak of celebrity nude photos apparently stolen from compromised iCloud accounts; and in the same month as the enormous breach of Sony Pictures that included leaked emails detailing movie star salaries.

A statement from the Israeli court said the 14 month sentence for Lederman, plus a fine of 15,000 shekels (about $4000), would be a deterrent to others considering hacking crimes.

The case should also serve as a warning and a reminder to all of us to secure our online accounts with strong passwords and two-factor authentication wherever possible.

Faceglória: Like Facebook But Without All That ’Sin’

Welcome to Faceglória, the Brazilian Evangelical take on social media that opts for Gospel music and billowing white clouds instead of the moral swamps our Facebook pages have turned into.

Here you will find no swearing.
No selfies in that skimpy little bikini, no revenge porn.
No erotic content whatsoever, for that matter, nor anything else that all of us ungodly Facebook "sinners" are into.
Don’t click "Like" - click "Amen!"

That’s not an exaggeration. Users don’t "Like" things on Faceglória. Here, you really do click "Amen."

As co-founder Attila Barros told AFP, the goal is simple:

We want to be morally and technically superior to Facebook.

In Brazil, the country with the world’s largest Catholic population and one in which Evangelicals are an increasing force, Facebook has proved to be simply too violent and porn-filled, he said:

On Facebook you see a lot of violence and pornography. That’s why we thought of creating a network where we could talk about God, love and to spread His word.

So three years ago, Barros and three colleagues who are similarly devout Christians decided there was a market opportunity for a cleaned-up version of Facebook.

The four were working at the mayor’s office in Ferraz de Vasconcelos, near Brazil’s financial capital, Sªo Paulo.

The mayor liked the idea so much, he gave them about $16,000 (about £10,200) out of his own money to set up a business, and thus was Faceglória born.

The social network immediately proved popular, garnering 100,000 users in its first month, the founders claim.

Anyone can sign up, but the site’s currently only offered in a Portuguese version.

But Acir dos Santos, the mayor of Ferraz de Vasconcelos, says they’re not stopping in Brazil: they’ve purchased the domain in English and "in all possible languages," and the team is hoping that a mobile app also helps to extend their reach worldwide:

In two years we hope to get to 10 million users in Brazil. In a month we have had 100,000 and in two we are expecting a big increase thanks to a mobile phone app.

To be one of those users, you have to watch your Ps and Qs. Actually, you have to watch your booze and your cigarettes, too, since selfies get scrutinized for possible removal.

Other things that face removal from a team of 20 volunteers that patrol the site: potentially risquØ selfies and bikini shots, and, of course, the aforementioned swearing.

In fact, there’s a list of about 600 forbidden words. Homosexual activity depicted in videos is also verboten.

This isn’t an uphill battle, by any means. One of the volunteers, Daiane Santos, told AFP that Faceglória users aren’t into erotic promenading:

Our public doesn’t publish these kinds of photos.

This isn’t the first social media site tailored to a given religion.

As the BBC reports, a social network for Muslims launched in 2013 and currently has around 329,000 members.

The site, named Ummaland, includes "extended privacy settings" for women and daily Islamic inspirational quotes.

At the time of its inception, co-founders Maruf Yusupov and Jamoliddin

Daliyev said that the site was based on Islamic values:

We are creating Ummaland on Islamic values, no small talk, no boasting, no gossiping and backbiting but focusing on the message that really matters. We encourage every user to ponder upon if the message they share will benefit Ummah [Arabic for "community"] or not. If not, it is better to be silent.

From a secular perspective, the treatment of erotica and gay content as "sinful" is increasingly unacceptable.

But the idea of a social media site that’s squeaky clean - one that bans boasting or gossip or revenge porn or other myriad forms of nasty - certainly has its appeal.

Can we look forward to someday seeing a whitewashed version of Facebook that’s not aimed at a particular religion and which doesn’t ostracize gay people but simply opts for silence over attacks on the community?

After all, in the US, gay people are making enormous strides in being accepted as an integral part of the community, covered by the Constitution to the same extent as all citizens.

If a secular version of a squeaky clean Facebook came into being, would such a presumably highly censored creature flourish?

Readers, would you pull yourself out of the swamp in favor of a version of Faceglória or Ummaland that caters to your religious, anti-religious, or secular values?

How To Anonymously Access Wi-Fi from 2.5 Miles Away Using This Incredible Device

Anonymity is something that seems next to impossible in this era of government surveillance. Even Tor and VPNs are no longer seem to be enough to protect user privacy. Once your IP address is discovered, your Game Over!

However, a method have been devised that not only allow users to anonymously connect to public Wi-Fi network, but also let them connect from about 2.5 Miles away.

Security researcher Benjamin Caudill has developed a device that adds an extra layer of anonymity to whistleblowers, journalists, dissidents and, of course, criminals.

Dubbed ProxyHam, it’s a "hardware proxy" that allows users to connect to a long-distance public Wi-Fi network over an unidentifiable low-frequency radio channels, making it more difficult for government agencies and spies to unearth the real identity and source of the Internet traffic.

Proxyham is comprised of a WiFi-enabled Raspberry Pi computer, along with a three antennas setup. One antenna is used to connect to a source Wi-Fi network at a public place, and the other two antennas are used to transmit the Wi-Fi signal at a 900 MHz frequency.

By relying on a 900 MegaHertz radio connection, ProxyHam effectively

connects to a far-away Wi-Fi, with a range of between 1 and 2.5 Miles, depending upon certain interference factors.

Therefore, in case if spies manage to completely trace the target’s internet connection, they will find only the IP address of ProxyHam box transmitting a low-level radio signal thousands of feet away in some direction.

Caudill tells Motherboard that he and his colleagues are also working to add additional features like self-destruction to the ProxyHam. Future iterations might be small enough as to fit Proxyham into a book to make it easier to hide.

"If you throw this in a library it would take you years to be able to identify it," Caudill said.

Caudill will unveil this game changer ProxyHam box at the Def Con hacker conference in Las Vegas next month. He will also release the hardware specs, the source code and the blueprint of the device so that anyone can develop their own.

Caudill is planning to sell ProxyHam at cost for $200, "as a service to the community," and he also hopes that he ll be able to drop the price to $150 soon.

Is GG1 The New Version of Google Glass?

Google appears to be testing a new version of Google Glass called GG1 after an unknown piece of Google hardware was logged by the US Federal Communications Commission (FFC).

The FFC, which tests electronic products to ensure they’re safe for human contact, logged an anonymous gadget codenamed A4R-GG1 the week, spotted by Droid Life.

While not a great deal was revealed about the gadget, it was not categorised as a tablet or smartphone, and was equipped with WiFi and Bluetooth capabilities alongside an inbuilt rechargeable battery.

It’s possible the mystery object is another wearable, after a series of adverts posted on Google’s website revealed the Google Glass team had changed its focus to developing smart eyewear and other related products .

The job listings include an Audio Hardware Manager, a Human Factors Designer, an RF Systems Engineer and a Hardware Automation Engineer (Manufacturing).

The description suggests that Google may be looking to expand Glass into a family of assorted wearable products, rather than the single head-mounted device that struggled to win over consumers.

Google withdrew the wearable headset from the market in January, but insisted it was planning to release a new version "when it’s ready". Despite many years in production, Glass was still officially a prototype when it went on sale in the UK last June for £1,000.

Concerns were raised over the ethics of using Google Glass in public after privacy groups argued the headset could be used for covert recording or photography.

Google published its own etiquette guide for users last February, advising them not be "creepy or rude" while wearing it and not to take pictures without permission.

Is Google Glass 2.0 Coming Soon?

Could the next version of Google Glass be close at hand?

Last week the Federal Communications Commission approved a new Google device called "GG1."

This new device is shrouded in mystery because Google was granted confidentiality. What we do know (thanks to Droid Life): The device has Wi-Fi, Bluetooh and a battery you cannot change.

In an emailed statement, Google said: "The team is heads down building the future of the product and isn’t giving interviews at the moment."

Google stopped selling the first version of Glass in January amid slow sales and shut down its Explorer program, putting Glass in a new unit under the stewardship of Tony Fadell, head of Google’s Nest connected home division.

Outgoing chief financial officer Patrick Pichette talked about Glass taking a "pause" during Google’s fourth-quarter conference call with analysts.

"When teams aren’t able to hit hurdles, but we think there is still a lot of promise, we might ask them to take a pause and take the time reset their strategy as we recently did in the case of Glass," Pichette said.

Executive Chairman Eric Schmidt has said Google plans to release new versions of Glass, maybe even this year. Google has also been hiring for Glass, leading some to speculate that Google is doubling down on wearable products. In April, the Wall Street Journal reported that Italian eyewear maker Luxottica is in a partnership to build the new version of Glass.

Glass chief Ivy Ross has said the updated version of Glass will be cheaper and have longer battery life, better sound quality and a sharper display.

It’s unclear how Google will grapple with perhaps the biggest challenge to mainstream adoption the social stigma especially as Glass takes on growing competition from Apple Watch and Microsoft’s new wearable technology HoloLens as well as a slew of other wearable rivals.

Some believe Google is not going to target consumers, but will instead focus on the market where Glass has seen the most success: enterprise.

Google Protects Gmail Users From Sending Regrettable Notes

Google is making it easier to steer clear of the trouble that can be caused by a misdirected or inappropriate email.

An option to cancel the delivery of an email within 30 seconds of hitting the send button is now a standard safeguard in Google's Gmail as part of a settings change made this week.

The "undo send" feature had already been available for the past six years in Google's experimental labs, but that required Gmail users taking extra steps to get it.

Gmail accountholders will now be able to activate the protection in Gmail's settings. The tool delays the delivery of emails from five to 30 seconds after the send button is pressed to give users a fleeting chance to retrieve an email mistakenly sent to the wrong person or an ill-conceived communique.

Google inserted the "undo send" feature last month into an email management application called "Inbox" designed for mobile devices.

Gmail, started 11 years ago, is the far more popular email service. It now boasts more than 900 million accountholders worldwide, according to statistics that Google released last month.

Facebook Locked Out Jemmaroid von Laalaa, So She Made It Her Real Name

Just ask Little Miss Hot Mess or Dana Lone Hill: Facebook's real-name policy has driven people nuts and/or off the social media network.

Now, besides the LGBT (lesbian/gay/bisexual/transgender) community or the Native Americans whose names have been dubbed fake, we might have yet another category of people losing access to their accounts: those who come up with stupid names in a bid to get security though obscurity.

Without further ado, say hello to Ms. Jemmaroid von Laalaa.

Yes, that's her real name.

Well, it is now, given that the former Ms. Jemma Rogers so desperately wants to get back her account that she changed her name to the dopey pseudonym she first cooked up years ago in order to stay anonymous.

She did so via deed poll, a legal document used in the UK and other countries to change one's name.

As The Independent reports, von Laalaa first set up her Facebook account in 2008.

She hadn't wanted to be pestered with requests from people she didn't want to be friends with, so she created the von Laalaa pseudonym.

Eventually, though, Facebook's real-name policy caught up to her - a policy that the social network's been tweaking since autumn, trying to appease the drag kings and queens, political activists and domestic abuse survivors, and others who've been shut out of their accounts after using non-conventional (for white Americans, at any rate) names.

The policy requires that Facebook users sign up for accounts with the name that appears on official documents, like their credit card or birth certificate.

Accordingly, the site contacted von Laalaa, then known outside of Facebook as Jemma Rogers, and requested proof of her name.

She told The Independent that she rushed to switch her bank cards over to the von Laalaa name, but it was too late: the next day, Facebook suspended her account.

With the lock-out, von Laalaa lost access to her pictures and messages. In trying to get back in, Rogers went so far as to officially change her name to the one on her Facebook account.

But even after adopting the daft name, Facebook still wouldn't let her back in.

Rather, she's been getting canned messages telling her that the company will "look into" her problem, she says.

The Independent quotes her:

I can't believe I'm stuck with this stupid name and I still can't get into my Facebook.

I know I've been a complete moron, but Facebook are being ridiculous. I've been locked out of my account for five weeks now and have lost all of my photos, messages and precious memories.

So many people set up accounts in fake names so random people can't add them or so they don't have to awkwardly decline requests from people they know but don't want to be 'friends' with.

But Facebook have been over the top, they should be able to tell it's a genuine account but just under a fake name, I can't believe I am being punished like this.

Ms. von Laalaa was simply trying to maintain her privacy on social media - not a bad idea at all, given what can be grave consequences of letting the internet eavesdrop on your social media posts.

There are plenty of people who will suggest that the only way to protect your privacy is to stay off Facebook completely, pseudonym or no.

In March, European Commission attorney Bernhard Schima advised EU citizens to close their Facebook accounts entirely if they want to keep their private information away from the prying eyes of US security services.

For those who choose to stick it out on Facebook, we've published plenty of tips on how to stay safer, and don't forget that you can always review your privacy settings with Facebook's new privacy checkup tool.

So no, Ms. von Laalaa/Rogers, you're not a moron.

But one of the things that she might have pondered before changing her name is whether or not deeds poll (and yes, that's the proper plural form of the term) are recognized in Facebook's homeland in the US - California, to be precise.

California, in fact, has two ways to change your name, at least technically.

One way is by common law - that’s when people simply adopt a new name that becomes legal via consistent use for business and personal affairs.

The other method is legal, with a court-ordered name change.

However, the Transgender Law Center advises people to go with the court order, given that few government agencies recognize common law name changes.

More to the point, though, is what a California court would think of a deed poll name change, if Ms. Von Laalaa decided to go the legal route to get her account back (she hasn’t mentioned that she would, and it likely won’t reach that level; the premise is just for hypothetical purposes).

According to the UK Deed Poll Office, you can use a deed poll as proof of your change of name outside the UK, but you’ll probably need to have it witnessed by a solicitor, and you also might need to have it legalized (which means having an apostille attached to it), depending on the organisation you’re trying to convince.

But regardless of whether Facebook recognizes a deed poll name change or wants a different type of legal vehicle, the fact is that there’s nothing pointing to these name-change methods having retrospective power, which is what von Laalaa seems to be after here.

Facebook has actually sought to be responsive to real-name predicaments while still trying to uphold a policy that aims for a homey, we-know-you’re-for-real feel, so there’s hope that Ms. Von Laalaa manages to get back into her account.

Then, hopefully, she can get back into her original name - though truth be told, I really adore her von Laalaa pseudonym!

Google Edges Closer to Spam-Free Gmail Experience

Google is edging even closer to a spam-free Gmail experience with the addition of new tools to help the existing spam filters weed out unwanted emails.

Google has nearly eradicated the problem already with less than 0.1 percent of email in the average Gmail inbox being spam, according to a blog post from Sri Harsha Somanchi, a Google product manager.

The addition of artificial neural network technology, which can be found in Google’s Now and Search apps, will hopefully ring the death knell for those annoying emails.

While Gmail’s filters can already learn when a user chooses the "Report spam" and "Not spam" buttons, it will be enhanced with artificial neural network technology, which can use machine learning to detect even the sneakiest of spam messages to make sure it doesn’t land in someone’s inbox.

The improvements make Gmail’s filter even better at finding phishing

emails that may appear to come from a trusted contact but aren’t actually legitimate, according to the blog post.

Google is also introducing a set of postmaster tools designed for people who send a lot of emails that could potentially be marked as spam when they aren’t.

"The Gmail Postmaster Tools help qualified high-volume senders analyze their email, including data on delivery errors, spam reports, and reputation. This way they can diagnose any hiccups, study best practices, and help Gmail route their messages to the right place," Somanchi wrote.

In other words: No more digging through your spam folder to find your favorite newsletter or an emailed receipt.

Spam Email Levels Drop to Lowest Point in a Decade

Spam email levels have dropped to a 12-year low, new data from security firm Symantec shows.

The overall spam email level has fallen below the 50 percent mark, putting spam levels on the same levels as they were in September 2003.

Levels dropped by 0.6 percentage points from May. By comparison, Kaspersky Lab said 59.2 percent of all email in the first quarter of this year was spam.

As big data, the IoT, and social media spread their wings, they bring new challenges to information security and user privacy.

But mining remains the industry most affected by spam with a 56 percent spam rate, second to manufacturing and construction, the report said.

Spam may be innocuous and annoying to many, but unwanted emails can come with attached malware and links that generate money when clicked.

The drop in spam and phishing related emails suggests cyberattackers are focusing their efforts on other ways to generate money. Malware-based attacks, and ransomware and crypto-ransomware - where files are locked and encrypted for a fee - are on the rise.

"This increase in activity lends more evidence to the idea that, with the continued drops in email-based malicious activity, attackers are simply moving to other areas of the threat landscape," said Symantec’s Ben Nahorney in the report.

In the past few years, police and law enforcement have continually targeted spam networks with take-downs and raids. But private industry, notably email providers like Google, have also begun working to reduce the amount of spam that reaches inboxes.

The search giant’s latest trick, dubbed machine learning, to determine which messages should be marked as spam is helping to keep less than 0.1 percent of email in the average Gmail inbox as spam.

=~=~=~=